

Quantum interactive proofs with weak error bounds

Tsuyoshi Ito*

Hirokata Kobayashi†

John Watrous*

Abstract

This paper proves that the computational power of quantum interactive proof systems, with a double-exponentially small gap in acceptance probability between the completeness and soundness cases, is precisely characterized by EXP, the class of problems solvable in exponential time by deterministic Turing machines. This fact, and our proof of it, has implications concerning quantum and classical interactive proof systems in the setting of unbounded error that include the following:

- Quantum interactive proof systems are strictly more powerful than their classical counterparts in the unbounded-error setting unless $\text{PSPACE} = \text{EXP}$, as even unbounded error classical interactive proof systems can be simulated in PSPACE.
- The recent proof of Jain, Ji, Upadhyay, and Watrous (STOC 2010) establishing $\text{QIP} = \text{PSPACE}$ relies heavily on the fact that the quantum interactive proof systems defining the class QIP have bounded error. Our result implies that some nontrivial assumption on the error bounds for quantum interactive proofs is unavoidable to establish this result (unless $\text{PSPACE} = \text{EXP}$).
- To prove our result, we give a quantum interactive proof system for EXP with perfect completeness and soundness error $1 - 2^{-2^{\text{poly}}}$, for which the soundness error bound is provably tight. This establishes another respect in which quantum and classical interactive proof systems differ, because such a bound cannot hold for any classical interactive proof system: distinct acceptance probabilities for classical interactive proof systems must be separated by a gap that is at least (single-)exponentially small.

We also study the computational power of a few other related unbounded-error complexity classes.

1 Introduction

Interactive proof systems [Bab85, GMR89] are a central notion in complexity theory. It is well-known that IP, the class of problems having single-prover classical interactive proof systems with polynomially-bounded verifiers, coincides with PSPACE [Fel86, LFKN92, Sha92], and it was recently proved that the same characterization holds when the prover and verifier have quantum computers [JJUW10]. More succinctly, it holds that

$$\text{IP} = \text{PSPACE} = \text{QIP}. \quad (1)$$

The two equalities in (1) are, in some sense, intertwined: it is only through the trivial relationship $\text{IP} \subseteq \text{QIP}$, together with the landmark result $\text{PSPACE} \subseteq \text{IP}$, that we know $\text{PSPACE} \subseteq \text{QIP}$. While there exist classical refinements [She92, Mei10] of the original method of Lund, Fortnow, Karloff, and Nisan [LFKN92] and Shamir [Sha92] used to prove $\text{PSPACE} \subseteq \text{IP}$, there is no “short-cut” known that proves $\text{PSPACE} \subseteq \text{QIP}$ through the use of quantum computation.

The opposite containments required to prove the two equalities in the above equation (1) are $\text{IP} \subseteq \text{PSPACE}$ and $\text{QIP} \subseteq \text{PSPACE}$, respectively. The first containment is usually attributed to Feldman [Fel86], and can fairly

*Institute for Quantum Computing and School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada.

†Principles of Informatics Research Division, National Institute of Informatics, Tokyo, Japan.

be described as being straightforward to prove. The standard proof, in fact, gives a polynomial-space algorithm that computes the optimal acceptance probability for a prover in a classical interactive proof system *exactly*, with this optimal probability expressible as some integer divided by 2^k , where k is the maximum number of coin-flips used by the verifier. The proof of the containment $\text{QIP} \subseteq \text{PSPACE}$ given in [JJUW10], on the other hand, is more complicated: it uses known properties of QIP [KW00, MW05] to derive a semidefinite programming formulation of it, which is then approximated in PSPACE through the use of an algorithm based on the *matrix multiplicative weights update* method [AK07, WK06]. Unlike the standard proof of $\text{IP} \subseteq \text{PSPACE}$, this proof depends crucially on the bounded-error property of the quantum interactive proof systems that define QIP.

There must, of course, be alternate ways to prove $\text{QIP} \subseteq \text{PSPACE}$, and we note that Wu [Wu10] and Gutoski and Wu [GW10] have made advances in both simplifying and extending the proof method of [JJUW10]. The main question that motivates the work we present in this paper is whether the assumption of bounded-error is *required* to prove $\text{QIP} \subseteq \text{PSPACE}$, or could be bypassed. Our results demonstrate that indeed *some* assumption on the gap between completeness and soundness probabilities must be in place to prove $\text{QIP} \subseteq \text{PSPACE}$ unless $\text{PSPACE} = \text{EXP}$.

To explain our results in greater detail it will be helpful to introduce the following notation. Given any choice of functions $m : \mathbb{N} \rightarrow \mathbb{N}$ and $a, b : \mathbb{N} \rightarrow [0, 1]$, where we take $\mathbb{N} = \{0, 1, 2, \dots\}$, we write $\text{QIP}(m, a, b)$ to denote the class of promise problems¹ $A = (A_{\text{yes}}, A_{\text{no}})$ having a quantum interactive proof system² with $m(|x|)$ messages, completeness probability at least $a(|x|)$ and soundness error at most $b(|x|)$ on all input strings $x \in A_{\text{yes}} \cup A_{\text{no}}$. When sets of functions are taken in place of m , a , or b , it is to be understood that a union is implied. For example,

$$\text{QIP}(\text{poly}, 1, 1 - 2^{-\text{poly}}) = \bigcup_{m, p \in \text{poly}} \text{QIP}(m, 1, 1 - 2^{-p}),$$

where *poly* denotes the set of all functions of the form $p : \mathbb{N} \rightarrow \mathbb{N}$ for which there exists a polynomial-time deterministic Turing machine that outputs $1^{p(n)}$ on input 1^n for all $n \in \mathbb{N}$. We will also frequently refer to functions of the form $f : \mathbb{N} \rightarrow [0, 1]$ that are polynomial-time computable, and by this it is meant that a polynomial-time deterministic Turing machine exists that, on input 1^n , outputs a rational number $f(n)$ in the range $[0, 1]$, represented by a ratio of integers expressed in binary notation. Our main result may now be stated more precisely as follows.

Theorem 1. *It holds that*

$$\bigcup_a \text{QIP}(\text{poly}, a, a - 2^{-2^{\text{poly}}}) = \text{QIP}(3, 1, 1 - 2^{-2^{\text{poly}}}) = \text{EXP},$$

where the union is taken over all polynomial-time computable functions $a : \mathbb{N} \rightarrow (0, 1]$.

The only new relation in the statement of Theorem 1 is

$$\text{EXP} \subseteq \text{QIP}(\text{poly}, 1, 1 - 2^{-2^{\text{poly}}}); \tag{2}$$

we have expressed the theorem in the above form only for the sake of clarity. In particular, the containment

$$\text{QIP}(\text{poly}, 1, 1 - 2^{-2^{\text{poly}}}) \subseteq \text{QIP}(3, 1, 1 - 2^{-2^{\text{poly}}})$$

¹We formulate decision problems as *promise problems* [ESY84] because using promise problems is more natural than restricting our attention to languages in the presence of error bounds.

²The definitions of quantum computational models based on quantum circuits, including quantum interactive proof systems, is particularly sensitive to the choice of a gate set in the unbounded error setting. For our main result we take the standard Toffoli, Hadamard, $\pi/2$ -phase-shift gate set, but relax this choice for a couple of our secondary results.

follows from the fact that

$$\text{QIP}(m, 1, 1 - \varepsilon) \subseteq \text{QIP}(3, 1, 1 - \varepsilon/(m - 1)^2)$$

for all $m \in \text{poly}$ and any function $\varepsilon : \mathbb{N} \rightarrow [0, 1]$, as was proved in [KKMV09] (or an earlier result of [KW00] with a slightly weaker parameter). The containment

$$\text{QIP}(3, 1, 1 - 2^{-2^{\text{poly}}}) \subseteq \bigcup_a \text{QIP}(\text{poly}, a, a - 2^{-2^{\text{poly}}})$$

is trivial. The containment

$$\bigcup_a \text{QIP}(\text{poly}, a, a - 2^{-2^{\text{poly}}}) \subseteq \text{EXP}$$

follows from the results of Gutoski and Watrous [GW07], as a semidefinite program representing the optimal acceptance probability of a given quantum interactive proof system³ can be solved to an exponential number of bits of accuracy using an exponential-time algorithm [Kha79, GLS88, NN94].

The new containment (2), which represents the main contribution of this paper, is proved in two steps. The first step constructs a classical two-prover one-round interactive proof system with one-sided error double-exponentially close to 1 for the EXP-complete **SUCCINCT CIRCUIT VALUE** problem. It will be proved that when an instance whose answer is “no” is given to this proof system, provers cannot make the verifier accept with probability more than double-exponentially close to 1 even if they are allowed to use a *no-signaling strategy*, i.e., a strategy that cannot be used for communication between them. The second step converts this classical two-prover one-round interactive proof system to a single-prover quantum interactive proof system without ruining its soundness properties.

Theorem 1 and its proof have the following three consequences.

- Unbounded-error quantum interactive proof systems are strictly more powerful than their classical counterparts unless $\text{PSPACE} = \text{EXP}$, as unbounded-error classical interactive proof systems recognize exactly PSPACE .
- The dependence on the error bound in the proof in [JJUW10] is not an artifact of the proof techniques, but is a necessity unless $\text{PSPACE} = \text{EXP}$. To be more precise, even though a double-exponential gap is sufficient to obtain the EXP upper bound by applying a polynomial-time algorithm for semidefinite programming, Theorem 1 implies that a double-exponential gap is not sufficient for the PSPACE upper bound unless $\text{PSPACE} = \text{EXP}$.
- Our proof of Theorem 1 shows that a quantum interactive proof system can have a completeness-soundness gap smaller than singly exponential, which cannot happen in classical interactive proof systems. In our quantum interactive proof system for EXP, the gap is double-exponentially small, and this is tight in the sense that a dishonest prover can make the verifier accept with probability double-exponentially close to 1.

We do not know if the double-exponentially small gap in Theorem 1 can be improved to one that is single-exponentially small by constructing a different proof system.

The two parts of the proof of Theorem 1 mentioned above are contained in Sections 2 and 3. Some additional results concerning unbounded-error quantum interactive proof systems are discussed in Section 4.

³The results of Gutoski and Watrous [GW07] establish an EXP upper bound even for interactive proof systems with two competing quantum provers, and only mild assumptions on the gate set are needed to obtain this containment. Namely, the containment holds if the gate set consists of finitely many gates and the Choi-Jamiołkowski representation of each gate is a matrix made of rational complex numbers.

2 A no-signaling proof system for EXP with a weak error bound

As discussed in the previous section, our proof of the containment (2) has two parts. This section discusses the first part, in which we present a classical two-prover one-round interactive proof system for an EXP-complete problem. The proof system will have perfect completeness and a soundness error double-exponentially close to 1, even when the provers are permitted to employ an arbitrary *no-signaling strategy*. No-signaling strategies, which are defined below, have been considered previously in [Hol09] and [IKM09], for instance.

2.1 Definition of no-signaling proof systems

In a (*classical*) *two-prover one-round interactive proof system*, a verifier is a randomized polynomial-time process having access to two provers (which we will call Alice and Bob). All of the parties are given the same input string x . The verifier produces polynomial-length questions to Alice and Bob, receives polynomial-length answers from them, and decides whether to accept or reject.

A verifier V naturally defines a family of two-player one-round games indexed by input strings. A (*classical*) *two-player one-round game* $G = (S, T, Y, Z, \pi, R)$ is determined by finite sets S, T, Y , and Z , a probability distribution π over $S \times T$ and a function $R: S \times T \times Y \times Z \rightarrow [0, 1]$. The value $R(s, t, y, z)$ is written as $R(y, z | s, t)$ by convention. This game is interpreted as a cooperative two-player game of imperfect information played by two *players* (Alice and Bob) and run by a third party called the *referee*, who enforces the rules. First the referee generates a pair of questions $(s, t) \in S \times T$ according to the probability distribution π and sends s to Alice and t to Bob. Then Alice responds to the referee with an element $y \in Y$ and Bob responds with $z \in Z$. Finally the referee decides whether Alice and Bob win or lose, using randomness in the most general situation: Alice and Bob win with probability $R(y, z | s, t)$ and lose with probability $1 - R(y, z | s, t)$. Note that if we fix a verifier and an input string $x \in \{0, 1\}^*$, the verifier acts as a referee in some two-player one-round game $G_{V,x}$.

A *strategy* of players in a two-prover one-round game $G = (S, T, Y, Z, \pi, R)$ is a family of probability distributions $p_{s,t}$ over $Y \times Z$ indexed by $(s, t) \in S \times T$, where the value $p_{s,t}(y, z)$ represents the probability with which Alice replies with the string y and Bob replies with the string z under the condition that the verifier sends the question s to Alice and the question t to Bob. It is customary to write $p(y, z | s, t)$ instead of $p_{s,t}(y, z)$. The strategy is said to be *no-signaling* if the following *no-signaling conditions* are satisfied:

1. No-signaling from Alice to Bob:

$$\sum_{y \in Y} p(y, z | s, t) = \sum_{y \in Y} p(y, z | s', t)$$

for all $s, s' \in S, t \in T$, and $z \in Z$.

2. No-signaling from Bob to Alice:

$$\sum_{z \in Z} p(y, z | s, t) = \sum_{z \in Z} p(y, z | s, t')$$

for all $s \in S, t, t' \in T$, and $y \in Y$.

For functions $a, b: \mathbb{N} \rightarrow [0, 1]$, a two-prover one-round interactive proof system with a verifier V is said to *recognize* a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ with no-signaling provers with completeness probability at least a and soundness error at most b if the corresponding games satisfy the following conditions:

- *Completeness*. For every $x \in A_{\text{yes}}$, there exists a no-signaling strategy for the game $G_{V,x}$ that makes the verifier accept with probability at least $a(|x|)$.

- *Soundness.* For every $x \in A_{\text{no}}$, every no-signaling strategy for the game $G_{V,x}$ makes the verifier accept with probability at most $b(|x|)$.

The class of promise problems A having such a two-prover one-round interactive proof system is denoted by $\text{MIP}_{a,b}^{\text{ns}}(2, 1)$. It is known that $\text{MIP}_{a,b}^{\text{ns}}(2, 1) = \text{PSPACE}$ for all polynomial-time computable functions $a, b : \mathbb{N} \rightarrow (0, 1]$ for which $a(n) - b(n) \geq 1/p(n)$ for some $p \in \text{poly}$ [IKM09, Ito10].

2.2 The proof system for EXP and its analysis

This section describes a (classical) two-prover one-round interactive proof system for EXP with perfect completeness (for uncorrelated honest provers) and soundness error double-exponentially close to 1 against arbitrary no-signaling provers. The proof system has the additional property that the verifier's questions to the two provers are uniformly generated random strings, which will be important in the next section.

For a Boolean circuit C with N gates g_0, g_1, \dots, g_{N-1} , where gate g_j is an input to gate g_i only if $j < i$, a pair (N, D) is called a *succinct representation* of C if D is a Boolean circuit that, given an integer $0 \leq i \leq N-1$, returns the kind of gate g_i (ZERO, ONE, AND, OR, or NOT) and the indices of gates from which the inputs to g_i come (if any). Note that a succinct representation of length n represents a Boolean circuit with at most 2^n gates. The **SUCCINCT CIRCUIT VALUE** problem is the following decision problem.

SUCCINCT CIRCUIT VALUE

Instance: A succinct representation of a Boolean circuit C with N gates whose fan-in is at most two and an integer $0 \leq k \leq N-1$.

Question: Does gate g_k have value 1?

The **SUCCINCT CIRCUIT VALUE** problem is EXP-complete (see, e.g., Theorem 3.31 of [DK00]). We will give a two-prover one-round interactive proof system for **SUCCINCT CIRCUIT VALUE** with the completeness and soundness conditions stated above.

Theorem 2. *The **SUCCINCT CIRCUIT VALUE** problem has a two-prover one-round interactive proof system with no-signaling provers with perfect completeness and soundness error $1 - 2^{-2^{p(n)}}$ for some $p \in \text{poly}$, i.e.,*

$$\text{SUCCINCT CIRCUIT VALUE} \in \text{MIP}_{1, 1-2^{-2^{\text{poly}}}}^{\text{ns}}(2, 1).$$

Moreover, for some constant $\alpha > 0$ and infinitely many input strings x , the soundness error of this proof system is at least $1 - 2^{-2^{|x|^\alpha}}$.

Idea. The idea for the protocol is simple. The honest provers hold the correct values of all gates in a circuit. These values have to satisfy exponentially many local constraints, and the verifier checks one of these local constraints chosen randomly. It turns out that the local constraints, together with the no-signaling conditions, are sufficient to restrict the value of each gate claimed by the provers to the correct value inductively, beginning from the constant gates and propagating from the inputs and the output of each gate, concluding the soundness.

Protocol. Without loss of generality we assume that N is a power of two by adding unused gates as necessary. The verifier chooses two integers $0 \leq s, t \leq N-1$ uniformly and independently. He sends s to Alice and t to Bob. Alice answers all the values of the input gates of g_s in the same order as D returns (if any). Bob answers the value of g_t . The verifier checks the following conditions.

- If $s = t$, then Bob's answer must be equal to the value computed from Alice's answers (if any) and the kind of gate g_s .

- (b) If g_t is an input to gate g_s , then the value of g_t claimed by Alice must agree with the value claimed by Bob.
- (c) If $t = k$, then Bob's answer must be 1.

The verifier accepts if and only if all the conditions (a)–(c) are satisfied.

Completeness. Completeness is easy: if the value of gate g_k is 1, then provers who simply answer the requested values of gates are accepted with probability 1.

Soundness. Now we shall prove that this two-prover interactive proof system has soundness error at most $1 - 2^{-O(N)} = 1 - 2^{-O(2^n)}$ against no-signaling dishonest provers. Again we can assume that N is a power of two without loss of generality.

Let (N, D, k) be an instance of **SUCCINCT CIRCUIT VALUE**, and let $v_i \in \{0, 1\}$ be the value of gate g_i for $0 \leq i \leq N - 1$. Fix any no-signaling strategy in the two-prover interactive proof system, and let ε be the probability that this strategy is rejected. We assume $\varepsilon < 1/(N^2 \cdot 3^N)$ and prove that gate g_k has value 1.

Let $\varepsilon(s, t)$ be the probability that this strategy is rejected, conditioned on pair (s, t) of questions. Then

$$\varepsilon = \frac{1}{N^2} \sum_{s, t} \varepsilon(s, t),$$

which implies for any questions s, t , it holds that

$$\varepsilon(s, t) \leq \sum_{s', t'} \varepsilon(s', t') = N^2 \varepsilon < \frac{1}{3^N}.$$

Let $\delta(i)$ be the probability that Bob answers $1 - v_i$ when asked i .

We prove that

$$\delta(i) < \frac{3^i}{3^N} \tag{3}$$

by induction on i .

First we consider the case where g_i is a constant gate. This includes the case of $i = 0$. As Bob gives a wrong answer with probability $\delta(i)$ when Bob's question is i , regardless of Alice's question, $\delta(i) \leq \varepsilon(i, i)$ by considering the probability that the strategy fails in the test (a), which implies

$$\delta(i) \leq \varepsilon(i, i) < \frac{1}{3^N} \leq \frac{3^i}{3^N}.$$

Suppose $i \geq 1$ and g_i is not a constant gate. Assume g_i is an AND or OR gate, and let j_1 and j_2 be the indices of the inputs to g_i . First consider Alice's answer in the case where her question is i . If the value of g_{j_1} claimed by Alice when her question is i is wrong, then when Bob's question is j_1 , either Bob's answer is wrong or Alice's and Bob's answers disagree. If their answers disagree, then the verifier rejects by the test (b), and therefore this happens with probability at most $\varepsilon(j_1, j_1) < 1/3^N$. As Bob's answer is wrong with probability $\delta(j_1)$ and their answers disagree with probability less than $1/3^N$, the value of g_{j_1} claimed by Alice when her question is i is wrong with probability at most

$$\delta(j_1) + \frac{1}{3^N} < \frac{3^{j_1} + 1}{3^N}.$$

In the same way, the value of g_{j_2} claimed by Alice when her question is i is wrong with probability at most

$$\delta(j_2) + \frac{1}{3^N} < \frac{3^{j_2} + 1}{3^N}.$$

If Bob's answer for i is wrong, then if both questions are i , at least one of the following happens:

- The value of g_{j_1} claimed by Alice is wrong. This happens with probability less than $(3^{j_1} + 1)/3^N$.
- The value of g_{j_2} claimed by Alice is wrong. This happens with probability less than $(3^{j_2} + 1)/3^N$.
- The values of g_{j_1} and g_{j_2} claimed by Alice are correct, but the value of g_i claimed by Bob is wrong. As this is detected by the test (a) of the verifier, it happens with probability at most $\varepsilon(i, i) < 1/3^N$.

Therefore,

$$\delta(i) < \frac{3^{j_1} + 1}{3^N} + \frac{3^{j_2} + 1}{3^N} + \frac{1}{3^N} < \frac{3^i}{3^N}.$$

The case where g_i is a NOT gate is proved in a similar way. This finishes the inductive case and establishes the inequality (3) for all i .

The inequality (3) implies that Bob's answer to question k is equal to v_k with probability greater than $1 - 3^k/3^N \geq 2/3$. On the other hand, by the test (c), Bob's answer to question k is equal to 1 with probability at least $1 - \varepsilon(k, k) > 1 - 1/3^N \geq 2/3$. These two conditions imply $v_k = 1$.

Remark. For a function $a: \mathbb{N} \rightarrow (0, 1]$, let $\text{MIP}_{a, < a}^{\text{ns}}(2, 1)$ denote the class of promise problems having a two-prover one-round interactive proof system with no-signaling provers with acceptance probability at least a and soundness error strictly less than a . Because the maximum acceptance probability for no-signaling provers can be computed exactly by solving an exponential-size linear program [Pre], we have $\text{MIP}_{a, < a}^{\text{ns}}(2, 1) \subseteq \text{EXP}$ for any polynomial-time computable function $a: \mathbb{N} \rightarrow (0, 1]$ by using any polynomial-time algorithm for linear programming [Kha79, Kar84]. Combined with Theorem 2, we have $\text{MIP}_{a, < a}^{\text{ns}}(2, 1) = \text{EXP}$ for any such a .

Tightness of soundness analysis. We shall prove the “moreover” part of Theorem 2: the double-exponential gap is tight for this protocol. This will be used in the next section to prove that the soundness error of the quantum interactive proof system for EXP that we construct is at least $1 - 2^{-2^{\text{poly}}}$ on infinitely many input strings.

This can be proved by studying the instance of the **SUCCINCT CIRCUIT VALUE** problem used by Trevisan and Xhafa [TX98].⁴ Let h be a positive integer. Consider a circuit C with $N = 2h + 2$ gates $g_0, g_1, \dots, g_{2h+1}$, where g_0 and g_1 are ZERO gates and, for $1 \leq i \leq h$, g_{2i} and g_{2i+1} are two identical OR gates whose inputs come from $g_{2(i-1)}$ and $g_{2(i-1)+1}$. Clearly this circuit C has a succinct representation of length polylogarithmic in h . Let $k = 2h - 1$.

Alice and Bob decide their answers as follows. First we describe each prover's marginal probability distribution. When Bob is asked either $2i$ or $2i + 1$ where $0 \leq i \leq h$, he answers 1 with probability $1/2^{h-i}$ and 0 with probability $1 - 1/2^{h-i}$. When Alice is asked $2i$ or $2i + 1$ where $1 \leq i \leq h$, she answers $(1, 0)$ and $(0, 1)$ each with probability $1/2^{h-i+1}$, and $(0, 0)$ with probability $1 - 2^{h-i}$. The joint distribution of their answers is defined as follows. In what follows, $(y_1, y_2; z)$ denotes that Alice's answer is (y_1, y_2) and Bob's answer is z .

- $s = t$, $\lfloor s/2 \rfloor = i \geq 1$: Alice and Bob answer $(1, 0; 1)$ and $(0, 1; 1)$ each with probability $1/2^{h-i+1}$, and $(0, 0; 0)$ with probability $1 - 1/2^{h-i}$.
- $\lfloor s/2 \rfloor = i \geq 1$, $t = 2(i - 1)$: Alice and Bob answer $(1, 0; 1)$ and $(0, 1; 0)$ each with probability $1/2^{h-i+1}$, and $(0, 0; 0)$ with probability $1 - 1/2^{h-i}$.
- $\lfloor s/2 \rfloor = i \geq 1$, $t = 2(i - 1) + 1$: Alice and Bob answer $(1, 0; 0)$ and $(0, 1; 1)$ each with probability $1/2^{h-i+1}$, and $(0, 0; 0)$ with probability $1 - 1/2^{h-i}$.
- Otherwise: Alice and Bob give their answers in any way as long as the marginal distributions agree with the description above (e.g. they answer independently).

⁴Note that we cannot avoid a large soundness error simply by restricting the problem to succinct Boolean formula values: with this restriction in place, the problem is in PSPACE [Lyn77].

It is easy to check that this strategy is no-signaling.

With this strategy, the verifier accepts unless $t \in \{0, 1\}$ and Bob answers 1 (which fails in test (a)). Therefore, the verifier accepts with probability at least $1 - 1/((h+1) \cdot 2^h) \geq 1 - 2^{-h} = 1 - 2^{-2^{n^\alpha}}$ for some constant $\alpha > 0$.

3 Simulating no-signaling provers with quantum interactive proofs

In this section we present the second part of the proof of the containment (2), which is a simulation of the two-prover one-round interactive proof system described in the previous section by a quantum interactive proof system with perfect completeness and unbounded soundness error. The result in this section can be stated as the following lemma.

Lemma 3. *Let $\varepsilon: \mathbb{N} \rightarrow (0, 1)$. Suppose that a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ has a two-prover one-round interactive proof system with no-signaling provers with perfect completeness and soundness error at most $1 - \varepsilon$. Assume moreover that, for each input $x \in A_{\text{yes}} \cup A_{\text{no}}$, the verifier's questions are chosen uniformly at random from the set $\{0, 1\}^{k(|x|)} \times \{0, 1\}^{k(|x|)}$, for some function $k \in \text{poly}$.*

- (i) *It holds that $A \in \text{QIP}(4, 1, 1 - \varepsilon^2/144)$, that is, the problem A has a four-message quantum interactive proof system with perfect completeness and soundness error at most $1 - \varepsilon^2/144$.⁵*
- (ii) *If the original system has soundness error $1 - \varepsilon'$ on input $x \in A_{\text{no}}$, then the derived quantum interactive proof system has soundness error at least $1 - \varepsilon'/4$ on input x .*

Note that the containment (2) follows by applying Lemma 3 to the two-prover one-round interactive proof system for the **SUCCINCT CIRCUIT VALUE** problem with no-signaling provers with perfect completeness and soundness error at most $1 - 2^{-2^{\text{poly}}}$ constructed in the previous section.

Construction of the protocol. Given an input string $x \in A_{\text{yes}} \cup A_{\text{no}}$, the verifier in the quantum interactive proof system that we construct acts as follows. First, the verifier prepares six quantum registers $S, T, S', T', Y,$ and Z in the state $|\Phi\rangle_{SS'}|\Phi\rangle_{TT'}|0\rangle_Y|0\rangle_Z$, where $|\Phi\rangle$ is the following maximally entangled state:

$$|\Phi\rangle = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right)^{\otimes k},$$

where $k = k(|x|)$. The four registers $S, T, S',$ and T' are k qubits long, and Y and Z must be long enough to hold Alice and Bob's answers in the two-prover one-round protocol. Next, in the first round, the verifier sends $S, T, Y,$ and Z to the prover and the prover sends back the same registers. Then, the verifier performs one of the following three tests each with probability $1/4$, and accepts unconditionally with probability $1/4$.

- *Simulation test:* The verifier measures $S', T', Y,$ and Z in the computational basis to obtain $s, t, y,$ and z , respectively. If the result is accepted by the base two-prover protocol, then the verifier accepts; otherwise he rejects.
- *Undo-Alice test:* The verifier tells the prover that the undo-Alice test is to be performed. He then sends registers S and Y back to the prover, and receives S . The verifier then destructively tests whether registers S and S' are in state $|\Phi\rangle$ or not. If they are, then he accepts; otherwise he rejects.

⁵It is possible to replace the coefficient $1/144$ with a larger constant at the expense of introducing slight complications in several parts in the proof, but we will choose to use simpler arguments rather than trying to maximize the coefficient.

- *Undo-Bob test:* The verifier tells the prover that the undo-Bob test is to be performed. He then sends registers T and Z back to the prover, and receives T . The verifier then destructively tests whether registers T and T' are in state $|\Phi\rangle$ or not. If they are, then he accepts; otherwise he rejects.

Note that this verifier can be implemented exactly with the standard Toffoli, Hadamard, $\pi/2$ -phase-shift gate set.

Proof of completeness and part (ii) of the lemma. Let $x \in A_{\text{yes}} \cup A_{\text{no}}$. We prove that if there exists a no-signaling strategy in the base two-prover interactive proof system that makes the verifier accept with probability $1 - \epsilon'$, then the quantum interactive proof system admits a strategy that makes the verifier accept with probability $1 - \epsilon'/4$.

Let p be the no-signaling strategy in the base two-prover interactive proof system whose acceptance probability is $1 - \epsilon'$. Let

$$p^A(y | s) = \sum_{z \in Z} p(y, z | s, t), \quad p^B(z | t) = \sum_{y \in Y} p(y, z | s, t)$$

be the marginal strategies, which are well-defined because of the no-signaling conditions. The prover in the constructed quantum interactive proof system performs the following. Registers \tilde{S} , \tilde{T} , \tilde{Y} , and \tilde{Z} are the prover's private registers initialized to $|0\rangle$.

- In the first round, he performs the following operation on registers \tilde{S} , \tilde{T} , \tilde{Y} , \tilde{Z} , and \tilde{Z} controlled on registers S and T being in the state $|s\rangle_S |t\rangle_T$:

$$|0\rangle_{\tilde{S}\tilde{T}\tilde{Y}\tilde{Z}\tilde{Z}} \mapsto |s\rangle_{\tilde{S}} |t\rangle_{\tilde{T}} \sum_{y,z} \sqrt{p(y, z | s, t)} |yy\rangle_{\tilde{Y}\tilde{Y}} |zz\rangle_{\tilde{Z}\tilde{Z}}.$$

This controlled operation changes the global state as follows:

$$\begin{aligned} & \frac{1}{2^k} \sum_{s,t} |ss0\rangle_{SS'\tilde{S}} |tt0\rangle_{TT'\tilde{T}} |00\rangle_{\tilde{Y}\tilde{Y}} |00\rangle_{\tilde{Z}\tilde{Z}} \\ & \mapsto \frac{1}{2^k} \sum_{s,t} |sss\rangle_{SS'\tilde{S}} |ttt\rangle_{TT'\tilde{T}} \sum_{y,z} \sqrt{p(y, z | s, t)} |yy\rangle_{\tilde{Y}\tilde{Y}} |zz\rangle_{\tilde{Z}\tilde{Z}}. \end{aligned}$$

- In the undo-Alice test, he performs the following operation on registers \tilde{S} , \tilde{Y} , and \tilde{Y} controlled on registers S , \tilde{T} , and \tilde{Z} being in the state $|s\rangle_S |t\rangle_{\tilde{T}} |z\rangle_{\tilde{Z}}$:

$$|s\rangle_{\tilde{S}} \sum_y \sqrt{\frac{p(y, z | s, t)}{p^B(z | t)}} |yy\rangle_{\tilde{Y}\tilde{Y}} \mapsto |0\rangle_{\tilde{S}} |00\rangle_{\tilde{Y}\tilde{Y}},$$

or does nothing if $p^B(z | t) = 0$. This controlled operation changes the global state to

$$\frac{1}{2^k} \sum_{s,t} |ss0\rangle_{SS'\tilde{S}} |ttt\rangle_{TT'\tilde{T}} |00\rangle_{\tilde{Y}\tilde{Y}} \sum_z \sqrt{p^B(z | t)} |zz\rangle_{\tilde{Z}\tilde{Z}},$$

which can be rewritten as

$$|\Phi\rangle_{SS'} |0\rangle_{\tilde{S}} |00\rangle_{\tilde{Y}\tilde{Y}} \otimes \frac{1}{\sqrt{2^k}} \sum_t |ttt\rangle_{TT'\tilde{T}} \sum_z \sqrt{p^B(z | t)} |zz\rangle_{\tilde{Z}\tilde{Z}}$$

by rearranging the registers.

- In the undo-Bob test, he performs the following operation on registers \tilde{T} , Z , and \tilde{Z} controlled on registers \tilde{S} , T , and \tilde{Y} being in the state $|s\rangle_{\tilde{S}}|t\rangle_T|y\rangle_{\tilde{Y}}$:

$$|t\rangle_{\tilde{T}} \sum_z \sqrt{\frac{p(y, z | s, t)}{p^A(y | s)}} |zz\rangle_{ZZ} \mapsto |0\rangle_{\tilde{T}}|00\rangle_{ZZ},$$

or does nothing if $p^A(y | s) = 0$. This controlled operation changes the global state to

$$\frac{1}{2^k} \sum_{s,t} |sss\rangle_{SS\tilde{S}} |tt0\rangle_{TT'\tilde{T}} |00\rangle_{ZZ} \sum_y \sqrt{p^A(y | s)} |yy\rangle_{Y\tilde{Y}},$$

which can be rewritten as

$$|\Phi\rangle_{TT'} |0\rangle_{\tilde{T}} |00\rangle_{ZZ} \otimes \frac{1}{\sqrt{2^k}} \sum_s |sss\rangle_{SS\tilde{S}} \sum_y \sqrt{p^A(y | s)} |yy\rangle_{Y\tilde{Y}}.$$

This strategy passes the undo-Alice and undo-Bob tests with certainty, and passes the simulation test with probability $1 - \varepsilon'$, resulting in the overall acceptance probability $1 - \varepsilon'/4$.

In particular, this implies that this quantum interactive proof system has perfect completeness and the statement in part (ii) of Lemma 3.

Proof of soundness. We prove the contrapositive: if there is a strategy in the single-prover protocol that is accepted with high probability, then the input must be a yes-instance. Fix an instance $x \in A_{\text{yes}} \cup A_{\text{no}}$ and a strategy in the single-prover protocol that is accepted with probability $1 - \varepsilon'$, where $\varepsilon' < \varepsilon(|x|)^2/144$. We prove that there is a no-signaling strategy for Alice and Bob in the base two-prover protocol that is accepted with probability at least $1 - 12\sqrt{\varepsilon'} > 1 - \varepsilon(|x|)$, implying that $x \in A_{\text{yes}}$. As the verifier accepts with probability $1 - \varepsilon'$, the simulation test, the undo-Alice test, and the undo-Bob test each succeed with probability at least $1 - 4\varepsilon'$.

Let register P denote the prover's private space. Without loss of generality, we assume that P is first initialized to $|0\rangle$ and that the prover performs a unitary operation $U = U_{STYZP}$ in the first round, a unitary operation $V = V_{SY\tilde{Y}P}$ in the second round in the undo-Alice test, and a unitary operation $W = W_{TZP}$ in the second round in the undo-Bob test. Let $|\Psi\rangle$ be the state in registers S , T , S' , T' , Y , Z , and P after the first round:

$$|\Psi\rangle = (I_{S'T'} \otimes U_{STYZP}) |\Phi\rangle_{SS'} |\Phi\rangle_{TT'} |0\rangle_Y |0\rangle_Z |0\rangle_P.$$

Let $\tilde{p}(s, t, y, z)$ be the probability with which the results of the measurement in the simulation test are s, t, y , and z :

$$\tilde{p}(s, t, y, z) = \langle s |_{S'} \langle t |_{T'} \langle y |_Y \langle z |_Z (\text{Tr}_{STP} |\Psi\rangle \langle \Psi|) | s \rangle_S | t \rangle_T | y \rangle_Y | z \rangle_Z.$$

Note that because the verifier never sends S' or T' to the prover, the reduced state $\text{Tr}_{STYZP} |\Psi\rangle \langle \Psi|$ is not affected by the operation by the prover in the first round. Therefore, $\text{Tr}_{STYZP} |\Psi\rangle \langle \Psi|$ is the completely mixed state $I/2^{2k}$ on S' and T' . This implies $\sum_{y,z} \tilde{p}(s, t, y, z) = 1/2^{2k}$ for every s and t . Let

$$p(y, z | s, t) = 2^{2k} \tilde{p}(s, t, y, z).$$

We shall show that strategy p is “close” to some no-signaling strategy. For this purpose, we use the notion of δ -no-signaling strategies.

A strategy p in a two-player one-round game is said to be δ -no-signaling with respect to probability distribution π over the questions if there exist single-prover strategies $p^A(y | s)$ and $p^B(z | t)$ such that

$$\sum_{s,t} \pi(s,t) \frac{1}{2} \sum_y \left| \sum_z p(y, z | s, t) - p^A(y | s) \right| \leq \delta, \quad (4)$$

$$\sum_{s,t} \pi(s,t) \frac{1}{2} \sum_z \left| \sum_y p(y, z | s, t) - p^B(z | t) \right| \leq \delta. \quad (5)$$

We will now prove that p is $4\sqrt{\varepsilon'}$ -no-signaling with respect to the uniform distribution over the questions. Toward this goal, we define

$$p^A(y | s) = \frac{1}{2^k} \sum_{t,z} p(y, z | s, t), \quad p^B(z | t) = \frac{1}{2^k} \sum_{s,y} p(y, z | s, t),$$

and prove the inequalities (4) and (5) with $\delta = 4\sqrt{\varepsilon'}$.

Let ρ be the state of registers S' , T , T' , and Y after the verifier receives a message from the prover in the undo-Bob test:

$$\rho = \text{Tr}_{\text{SZP}}(I_{SS'T'Y} \otimes W_{\text{TZP}}) |\Psi\rangle\langle\Psi| (I_{SS'T'Y} \otimes W_{\text{TZP}}^*).$$

The fact that this strategy passes the undo-Bob test with probability at least $1 - 4\varepsilon'$ can be written as

$$1 - \langle \Phi |_{\text{TT}'} (\text{Tr}_{S'Y} \rho) | \Phi \rangle_{\text{TT}'} \leq 4\varepsilon'.$$

We use the following easy lemma, which will be proved at the end of this section. In what follows, $\|X\|_1$ denotes the trace norm of a matrix X : $\|X\|_1 = \text{Tr} \sqrt{X^* X}$.

Lemma 4. *Let \mathcal{X} and \mathcal{Y} be finite-dimensional Hilbert spaces. Then, for a pure state $|\varphi\rangle \in \mathcal{X}$ and a density matrix ρ on $\mathcal{X} \otimes \mathcal{Y}$, it holds that*

$$\|\rho - |\varphi\rangle\langle\varphi| \otimes \text{Tr}_{\mathcal{X}} \rho\|_1 \leq 4\sqrt{1 - \langle\varphi|(\text{Tr}_{\mathcal{Y}} \rho)|\varphi\rangle}.$$

By Lemma 4, we have that

$$\|\rho - |\Phi\rangle\langle\Phi|_{\text{TT}'} \otimes \text{Tr}_{\text{TT}'} \rho\|_1 \leq 4\sqrt{4\varepsilon'} = 8\sqrt{\varepsilon'}.$$

Take the partial trace over T and note that $\text{Tr}_T \rho = \text{Tr}_{\text{STZP}} |\Psi\rangle\langle\Psi|$ to obtain that

$$\left\| \text{Tr}_{\text{STZP}} |\Psi\rangle\langle\Psi| - \frac{I_{T'}}{2^k} \otimes \text{Tr}_{\text{STT'ZP}} |\Psi\rangle\langle\Psi| \right\|_1 \leq 8\sqrt{\varepsilon'}.$$

Note that

$$\begin{aligned} \sum_z p(y, z | s, t) &= 2^{2k} \langle s |_{S'} \langle t |_{T'} \langle y |_Y (\text{Tr}_{\text{STZP}} |\Psi\rangle\langle\Psi|) | s \rangle_{S'} | t \rangle_{T'} | y \rangle_Y, \\ p^A(y | s) &= 2^k \langle s |_{S'} \langle y |_Y (\text{Tr}_{\text{STT'ZP}} |\Psi\rangle\langle\Psi|) | s \rangle_{S'} | y \rangle_Y. \end{aligned}$$

Then,

$$\begin{aligned}
& \frac{1}{2^{2k}} \sum_{s,t} \frac{1}{2} \sum_y \left| \sum_z p(y, z | s, t) - p^A(y | s) \right| \\
&= \frac{1}{2} \sum_{s,t,y} \left| \langle s |_{S'} \langle t |_{T'} \langle y |_Y \left(\text{Tr}_{\text{STZP}} |\Psi\rangle \langle \Psi| - \frac{I_{T'}}{2^k} \otimes \text{Tr}_{\text{STT'ZP}} |\Psi\rangle \langle \Psi| \right) | s \rangle_{S'} | t \rangle_{T'} | y \rangle_Y \right| \\
&\leq \frac{1}{2} \left\| \text{Tr}_{\text{STZP}} |\Psi\rangle \langle \Psi| - \frac{I_{T'}}{2^k} \otimes \text{Tr}_{\text{STT'ZP}} |\Psi\rangle \langle \Psi| \right\|_1 \\
&\leq 4\sqrt{\varepsilon'},
\end{aligned}$$

and therefore the inequality (4) is satisfied. The proof of the inequality (5) is analogous. This establishes the claim that strategy p is $4\sqrt{\varepsilon'}$ -no-signaling.

Now we prove that a δ -no-signaling strategy is close to some no-signaling strategy. We use a property of the no-signaling conditions shown by Holenstein [Hol09]. By applying Lemma 9.4 in [Hol09] twice, we obtain the following.

Lemma 5. *Let p be a δ -no-signaling strategy with respect to a probability distribution π . Then there exists a no-signaling strategy \hat{p} such that*

$$\sum_{s,t} \pi(s, t) \frac{1}{2} \sum_{y,z} |p(y, z | s, t) - \hat{p}(y, z | s, t)| \leq 2\delta.$$

The proof of Lemma 5 is the same as that of Lemma 9.5 in [Hol09], and is omitted.

By Lemma 5, there exists a no-signaling strategy \hat{p} such that

$$\frac{1}{2^{2k}} \sum_{s,t} \frac{1}{2} \sum_{y,z} |p(y, z | s, t) - \hat{p}(y, z | s, t)| \leq 8\sqrt{\varepsilon'}.$$

As the simulation test succeeds with probability at least $1 - 4\varepsilon'$, the no-signaling strategy \hat{p} makes the verifier in the base two-prover protocol accept with probability at least

$$1 - 4\varepsilon' - 8\sqrt{\varepsilon'} \geq 1 - 12\sqrt{\varepsilon'} > 1 - \varepsilon(|x|).$$

By the soundness of the base two-prover protocol, it must hold that $x \in A_{\text{yes}}$. Therefore, the quantum interactive proof has soundness error at most $1 - \varepsilon^2/144$.

In the rest of the section, we will prove Lemma 4. We use the following variant of Winter's gentle measurement lemma [Win99], proved by Ogawa and Nagaoka [ON07].

Lemma 6. *Let \mathcal{H} be a finite-dimensional Hilbert space. For a density matrix ρ on \mathcal{H} and a Hermitian matrix A on \mathcal{H} such that both A and $I_{\mathcal{H}} - A$ are positive semidefinite, it holds that*

$$\|\rho - \sqrt{A} \rho \sqrt{A}\|_1 \leq 2\sqrt{\text{Tr} \rho(I_{\mathcal{H}} - A)}.$$

Proof of Lemma 4. Let $Y = (\langle \varphi | \otimes I_Y) \rho (| \varphi \rangle \otimes I_Y)$, and let $A = | \varphi \rangle \langle \varphi | \otimes I_Y$. Then, it holds that

$$\begin{aligned}
\sqrt{A} \rho \sqrt{A} &= A \rho A = | \varphi \rangle \langle \varphi | \otimes Y, \\
\text{Tr} \rho A &= \langle \varphi | (\text{Tr}_Y \rho) | \varphi \rangle.
\end{aligned}$$

By Lemma 6, it holds that

$$\|\rho - |\varphi\rangle\langle\varphi| \otimes Y\|_1 \leq 2\sqrt{1 - \langle\varphi|(\text{Tr}_Y \rho)|\varphi\rangle}.$$

which implies that

$$\|\text{Tr}_X \rho - Y\|_1 \leq 2\sqrt{1 - \langle\varphi|(\text{Tr}_Y \rho)|\varphi\rangle}.$$

Then we have that

$$\begin{aligned} & \|\rho - |\varphi\rangle\langle\varphi| \otimes \text{Tr}_X \rho\|_1 \\ & \leq \|\rho - |\varphi\rangle\langle\varphi| \otimes Y\|_1 + \| |\varphi\rangle\langle\varphi| \otimes \text{Tr}_X \rho - |\varphi\rangle\langle\varphi| \otimes Y \|_1 \\ & = \|\rho - |\varphi\rangle\langle\varphi| \otimes Y\|_1 + \|\text{Tr}_X \rho - Y\|_1 \\ & \leq 4\sqrt{1 - \langle\varphi|(\text{Tr}_Y \rho)|\varphi\rangle}. \end{aligned}$$

□

4 Additional results

In this section we mention some additional results about quantum interactive proof systems with unbounded error.

4.1 One-round quantum interactive proofs for PSPACE with a weak error bound

Theorem 7. *It holds that $\text{PSPACE} \subseteq \text{QIP}(2, 1, 1 - 2^{-\text{poly}})$.*

Proof. The SUCCINCT BIPARTITENESS problem is the problem of deciding if an exponential-size graph, given in its succinct representation, is bipartite. It is known to be PSPACE-complete [LB89]. It is straightforward to construct a two-prover one-round XOR interactive proof system with perfect completeness and an exponentially small gap for this problem. (We refer the reader to [CHTW04, Weh06] for the definition of XOR interactive proof systems.) This proves the containment

$$\text{PSPACE} \subseteq \oplus\text{MIP}_{1,1-2^{-\text{poly}(n)}}[2].$$

Theorem 5.10 of Cleve, Høyer, Toner, and Watrous [CHTW04] implies that

$$\oplus\text{MIP}_{1,1-2^{-\text{poly}(n)}}[2] = \oplus\text{MIP}_{1,1-2^{-\text{poly}(n)}}^*[2],$$

and the construction of Wehner [Weh06] implies

$$\oplus\text{MIP}_{1,1-2^{-\text{poly}(n)}}^*[2] \subseteq \text{QIP}(2, 1, 1 - 2^{-\text{poly}}).$$

We obtain the theorem by chaining these inclusions. □

4.2 Upper bounds

One may also consider the power of quantum interactive proof systems when acceptance is defined by a sharp threshold value. That is, for any choice of functions $m \in \text{poly}$ and $a: \mathbb{N} \rightarrow (0, 1]$, we may consider the class $\text{QIP}(m, a, < a)$, defined as the class of promise problems $A = (A_{\text{yes}}, A_{\text{no}})$ having a quantum interactive proof system with $m(|x|)$ messages that accepts with probability at least $a(|x|)$ on inputs $x \in A_{\text{yes}}$, and with probability strictly smaller than $a(|x|)$ on all inputs $x \in A_{\text{no}}$. The notation $\text{QMA}(1, < 1)$ is shorthand for $\text{QIP}(1, 1, < 1)$. The following two theorems concerning these classes are proved.

In this section, the following mild assumptions are made on the gate set:

- The gate set consists of a finite number of gates.
- The amplitudes of each gate in the gate set are algebraic numbers.

Without the second restriction, even BQP would contain some undecidable languages; see Theorem 5.1 of Adleman, Demarrais, and Huang [ADH97].

4.2.1 Upper bound on $\text{QIP}(\text{poly}, a, < a)$

Theorem 8. *For any polynomial-time computable function $a : \mathbb{N} \rightarrow (0, 1]$, it holds that*

$$\text{QIP}(\text{poly}, a, < a) \subseteq \text{EXPSPACE}.$$

As stated in the introduction, Gutoski and Watrous [GW07] give a semidefinite program representing the optimal acceptance probability of a given quantum interactive proof system. When applied to the class $\text{QIP}(\text{poly}, a, < a)$, with our relaxed assumptions on the gate set, this transformation results in a semidefinite program of exponential size with algebraic coefficients. The remaining task is to decide whether this semidefinite program has the optimal value at least a or less than a . This task can be formulated as an exponential-size instance of the SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS problem.

SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS is a problem based on semidefinite programming. Let \mathbb{Q} , \mathbb{R} , and $\bar{\mathbb{Q}} \cap \mathbb{R}$ be the fields of rational numbers, real numbers, and algebraic real numbers, respectively. Each element α of $\bar{\mathbb{Q}} \cap \mathbb{R}$ can be encoded as a triple $(f(X), a, b)$ of the minimum polynomial $f(X)$ of α over \mathbb{Q} and $a, b \in \mathbb{Q}$ with $a < \alpha < b$ such that α is the only root of $f(X)$ between a and b . (See Section 10.2 of Basu, Pollack, and Roy [BPR03].)

SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS

Instance: Integers $n, d > 0$, m algebraic real matrices A_1, \dots, A_m of size $d \times d$, and m algebraic real numbers b_1, \dots, b_m .

Question: Does there exist a $d \times d$ real matrix $X \succeq 0$ such that $\text{Tr } A_i X = b_i$ for all i ?

The complexity of SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS is not known. (See Ramana [Ram97] for related results.) Although there exist polynomial-time algorithms for semidefinite programming that compute an approximate solution to an arbitrary precision, they cannot be applied in a straightforward way to the SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS problem. We point out that the problem is in PSPACE by using the following result.

Theorem 9 (Canny [Can88]). *The problem EXISTENTIAL THEORY OF THE REALS is in PSPACE. That is, given a quantifier-free Boolean formula $F(x_1, \dots, x_k)$ with atomic predicates of the forms $p(x_1, \dots, x_k) = 0$ and $p(x_1, \dots, x_k) > 0$, where p is a polynomial with integer coefficients given as a list of coefficients in binary notation, it is decidable in space polynomial in the length of the formula F whether there exists $(x_1, \dots, x_k) \in \mathbb{R}^k$ that satisfies F .*

Corollary 10. *The problem SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS is in PSPACE.*

Proof. Note that an algebraic number encoded as $(f(X), a, b)$ can be represented as a variable x constrained as $f(x) = 0 \wedge x - a > 0 \wedge b - x > 0$. By using this, we can write down each linear constraint $\text{Tr } A_i X = b_i$ in terms of the variables representing the d^2 coordinates of X . Moreover, the semidefinite constraint $X \succeq 0$ can be written as $\exists M. X = M^T M$, and therefore can be written as polynomial constraints on the coordinates of X . \square

By combining the semidefinite programming formulation of [GW07] and the polynomial-space algorithm for SEMIDEFINITE FEASIBILITY WITH ALGEBRAIC COEFFICIENTS, we obtain Theorem 8.

4.2.2 Upper bound on $\text{QMA}(1, < 1)$

Theorem 11. *It holds that $\text{QMA}(1, < 1) \subseteq \text{PSPACE}$.*

Proof. Let $L \in \text{QMA}(1, < 1)$. The same technique as the proof of $\text{QMA} \subseteq \text{PP}$ by Marriott and Watrous [MW05] reduces L to a problem of deciding whether or not an implicitly given exponential-sized matrix A has an eigenvalue 1, or equivalently $I - A$ is singular.

The entries of A are in a field F that depends on the language L as follows. Let $\alpha_1, \dots, \alpha_u \in \mathbb{C}$ be the distinct numbers that appear as entries in the natural representations of the gates in the gate set used by the verifier in the system for the language L . Let $F = \mathbb{Q}(\alpha_1, \dots, \alpha_u)$ be the field generated by the adjunction of $\alpha_1, \dots, \alpha_u$ to the field \mathbb{Q} , i.e. the smallest field containing all the rational numbers and $\alpha_1, \dots, \alpha_u$. Because $\alpha_1, \dots, \alpha_u$ are algebraic, F is a finite extension of the field \mathbb{Q} . By the primitive element theorem (see e.g. Problem 7.5 of [Lor06]), there exists an algebraic number $\alpha \in F$ such that $F = \mathbb{Q}(\alpha)$. Let $f(t)$ be the minimal polynomial of α over \mathbb{Q} and d be the degree of $f(t)$. The field F is isomorphic to the quotient field $\mathbb{Q}[t]/(f(t))$, by which we identify F with the set of polynomials over \mathbb{Q} of degree at most $d - 1$. Using this representation, addition, subtraction, multiplication, division, and equality testing of the numbers in F can be performed in NC.

Using this representation, each entry of A can be computed in PSPACE. Csanky's algorithm [Csa76] can then be used to determine whether $I - A$ is singular or not in PSPACE. \square

5 Open problems

We conclude with a short list of open problems related to quantum interactive proof systems with an unbounded error.

- Is $\text{EXP} \subseteq \text{QIP}(2, 1, < 1)$?
- We have $\text{PSPACE} \subseteq \text{QIP}(\text{poly}, 1, 1 - 2^{-\text{poly}}) \subseteq \text{EXP}$. Where does $\text{QIP}(\text{poly}, 1, 1 - 2^{-\text{poly}})$ lie? One may try to prove $\text{QIP}(\text{poly}, 1, 1 - 2^{-\text{poly}}) = \text{PSPACE}$ by improving the dependence of the parallel time of an approximation algorithm for semidefinite programming on the error parameter. Note, however, that this is open even for the special case of positive linear programming [TX98].
- Is it possible to improve our upper bound of EXPSPACE on $\text{QIP}(\text{poly}, a, < a)$? In particular, is it possible to avoid resorting to the exact feasibility of a semidefinite program? Or does the succinct version of the semidefinite feasibility problem belong to $\text{QIP}(\text{poly}, a, < a)$? How small can the gap in acceptance probability between the completeness case and the soundness case be in a quantum interactive proof system?
- Does the containment $\text{QMA} \subseteq \text{PP}$ [MW05] extend to the unbounded-error case? Our upper bound of PSPACE may not hold if perfect completeness is not assumed.

Acknowledgments

We thank the anonymous reviewers of an earlier version of this paper for helpful comments. Tsuyoshi Ito acknowledges support from NSERC, CIFAR, QuantumWorks, MITACS, CFI, and ORF. Hirotada Kobayashi is partially supported by the Grant-in-Aid for Scientific Research (B) No. 21300002 of the Japan Society for the Promotion of Science. John Watrous acknowledges support from NSERC, CIFAR, and MITACS.

References

- [ADH97] Leonard M. Adleman, Jonathan Demarrais, and Ming-Deh A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, October 1997.
- [AK07] Sanjeev Arora and Satyen Kale. A combinatorial, primal-dual approach to semidefinite programs. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 227–236, June 2007.
- [Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 496–505, May 1985.
- [BPR03] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer, 2003.
- [Can88] John Canny. Some algebraic and geometric computations in PSPACE. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 460–467, May 1988.
- [CHTW04] Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Proceedings: Nineteenth Annual IEEE Conference on Computational Complexity*, pages 236–249, June 2004.
- [Csa76] Laszlo Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976.
- [DK00] Ding-Zhu Du and Ker-I Ko. *Theory of Computational Complexity*. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 2000.
- [ESY84] Shimon Even, Alan L. Selman, and Yacov Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, May 1984.
- [Fel86] Paul Feldman. The optimum prover lives in PSPACE. Manuscript, 1986.
- [GLS88] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer, 1988.
- [GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, February 1989.
- [GW07] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 565–574, June 2007.
- [GW10] Gus Gutoski and Xiaodi Wu. Short quantum games characterize PSPACE, November 2010. Available as arXiv.org e-Print 1011.2787v1 [quant-ph].
- [Hol09] Thomas Holenstein. Parallel repetition: Simplifications and the no-signaling case. *Theory of Computing*, 5(Article 8):141–172, July 2009.
- [IKM09] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proceedings: Twenty-Fourth Annual IEEE Conference on Computational Complexity*, pages 217–228, July 2009.

- [Ito10] Tsuyoshi Ito. Polynomial-space approximation of no-signaling provers. In *Automata, Languages and Programming: Thirty-Seventh International Colloquium, Part I*, pages 140–151, July 2010.
- [JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. In *Proceedings of the Forty-Second Annual ACM Symposium on Theory of Computing*, pages 573–582, June 2010.
- [Kar84] Narendra Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica*, 4(4):373–395, December 1984.
- [Kha79] Leonid G. Khachiyan. A polynomial algorithm in linear programming. *Soviet Mathematics Doklady*, 20(1):191–194, 1979.
- [KKMV09] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18(2):273–307, June 2009.
- [KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, May 2000.
- [LB89] Antonio Lozano and José L. Balcázar. The complexity of graph problems for succinctly represented graphs. In *Graph-Theoretic Concepts in Computer Science*, volume 411 of *Lecture Notes in Computer Science*, pages 277–286, June 1989.
- [LFKN92] Carsten Lund, Lance Fortnow, Howard J. Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, October 1992.
- [Lor06] Falko Lorenz. *Algebra, Volume I: Fields and Galois Theory*. Universitext. Springer, 2006.
- [Lyn77] Nancy Lynch. Log space recognition and translation of parenthesis languages. *Journal of the ACM*, 24(4):583–590, October 1977.
- [Mei10] Or Meir. IP = PSPACE using error correcting codes. Technical Report TR10-137, revision #5, Electronic Colloquium on Computational Complexity, October 2010.
- [MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, June 2005.
- [NN94] Yurii Nesterov and Arkadii Nemirovskii. *Interior-Point Polynomial Algorithms in Convex Programming*, volume 13 of *SIAM Studies in Applied Mathematics*. SIAM, 1994.
- [ON07] Tomohiro Ogawa and Hiroshi Nagaoka. Making good codes for classical-quantum channel coding via quantum hypothesis testing. *IEEE Transactions on Information Theory*, 53(6):2261–2266, June 2007.
- [Pre] Daniel Preda. Private communication.
- [Ram97] Motakuri V. Ramana. An exact duality theory for semidefinite programming and its complexity implications. *Mathematical Programming*, 77(1):129–162, April 1997.
- [Sha92] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, October 1992.

- [She92] Alexander Shen. $IP = PSPACE$: Simplified proof. *Journal of the ACM*, 39(4):878–880, October 1992.
- [TX98] Luca Trevisan and Fatos Xhafa. The parallel complexity of positive linear programming. *Parallel Processing Letters*, 8(4):527–533, December 1998.
- [Weh06] Stephanie Wehner. Entanglement in interactive proof systems with binary answers. In *Twenty-Third Annual Symposium on Theoretical Aspects of Computer Science*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171, February 2006.
- [Win99] Andreas Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, November 1999.
- [WK06] Manfred K. Warmuth and Dima Kuzmin. Online variance minimization. In *Proceedings of the Nineteenth Annual Conference on Learning Theory*, volume 4005 of *Lecture Notes in Computer Science*, pages 514–528. Springer, June 2006.
- [Wu10] Xiaodi Wu. Equilibrium value method for the proof of $QIP = PSPACE$. Available as arXiv.org e-Print 1004.0264v3 [quant-ph], September 2010.